IN THE CLAIMS:

1. (Currently Amended) A method for certificate generation that enables efficient revocation of said certificate, comprising:

at a first node:

receiving a request to issue a certificate on behalf of a principal; and

forwarding said request to a second node, wherein said request includes a first identifier that identifies the first node; and

at the second node:

in response to receipt of the request, generating a certificate that includes said first identifier.

2. (Original) The method of claim 1 wherein said request further includes a second identifier that identifies a principal.

3. (Original) The method of claim 2 wherein said certificate further includes a public key associated with said principal, and said second identifier.

4. (Previously Presented) The method of claim 1 further including authenticating said certificate by said second node.

5. (Previously Presented) The method of claim 4 wherein authenticating said certificate comprises generating a certificate digitally signed by said second node.

6. (Previously Presented) The method of claim 5 wherein generating said certificate signed by said second node comprises generating a certificate digitally signed by said second node using a private key of a public private key pair associated with said second node.

7. (Original) The method of claim 1 wherein said certificate further includes a time stamp that identifies a time associated with the request.

8. (Previously Presented) The method of claim 1 further including authenticating said request by said first node.

9. (Previously Presented) The method of claim 8 wherein authenticating said request by said first node comprises digitally signing said request.

10. (Previously Presented) The method of claim 9 wherein digitally signing said request comprises the step of digitally signing said request using a private key of a public/private key pair associated with said first node.

11. (Original) The method of claim 1 wherein said certificate further includes a time stamp that is associated with a time and date when said request was received by said second node.

12-16. (Withdrawn)

17. (Currently Amended) A certification authority comprising:

a memory containing a computer program for generating a certificate that enables efficient revocation of said certificate; and

a processor operative to execute said computer program, said computer program containing program code for:

receiving a request from a registration authority to issue a certificate on behalf of a principal; and

in response to receipt of said request, generating said certificate that includes at least a registration authority identifier associated with said registration authority.

18. (Original) The certification authority of claim 17 wherein said request to issue said certificate is an authenticated request and said computer program further includes program code for verifying said authenticated request.

19. (Previously Presented) The certification authority of claim 17 wherein said certificate generated by said computer program further includes a principal identifier associated with said principal and a key associated with said principal.

20. (Original) The certification authority of claim 17 wherein said computer program further includes program code for storing within said certificate a time stamp associated with a time when said certification authority received said request from said registration authority.

21-27. (Withdrawn)

28. (Currently Amended) A computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for generating a certificate that enables efficient revocation of said certificate, said computer program being executable by a processor and comprising:

program code for receiving a request from a registration authority to issue a certificate on behalf of a principal; and

program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority wherein said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority.

29. (Original) The computer program product of claim 28 wherein said program code for generating said certificate is further operative to include within said certificate a time stamp associated with a time or receipt by said certification authority of said request from said registration authority of said request to issue said certificate.

30. (Currently Amended) A computer data signal, said computer data signal including a computer program for use in generating a certificate that enables efficient revocation of said certificate, said computer program comprising:

program code for receiving a request from a registration authority to issue a certificate on behalf of a principal; and

program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority wherein said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority.

31. (Original) The computer data signal of claim 30 wherein said program code for generating said certificate is operative to include within said certificate a time stamp associated with a time of receipt by said certification authority from said registration authority of said request to issue said certificate.

32. (Original) The computer data signal of claim 30 wherein said computer program further includes program code for publishing said certificate.

33. (Previously Presented) The computer data signal of claim 32 wherein said program code for publishing said certificate includes program code for forwarding said certificate to a directory server.

34. (Currently Amended) An apparatus for generating a certificate in a computer network, wherein said generating of said certificate enables efficient revocation of said certificate, the apparatus comprising:

means operative in response to receipt of a request from a first node coupled to said computer network at a second node coupled to said computer network for generating at said second node a certificate on behalf of a principal that includes a first node identifier associated with said first node.

35. (Currently Amended) The apparatus of claim 34 wherein said request was initiated by ~~a~~ said principal and said request includes a principal identifier associated with said principal and said certificate further includes said principal identifier and a public key associated with said principal.

36. (Original) The apparatus of claim 34 wherein said certificate is authenticated by said second node.

37. (Previously Presented) The apparatus of claim 34 further including means for comparing said first node identifier to a node identifier associated with an untrustworthy node on said network that is included within a certificate revocation list and providing an indication that said certificate is untrustworthy in the event said first node identifier matches said untrustworthy node identifier.